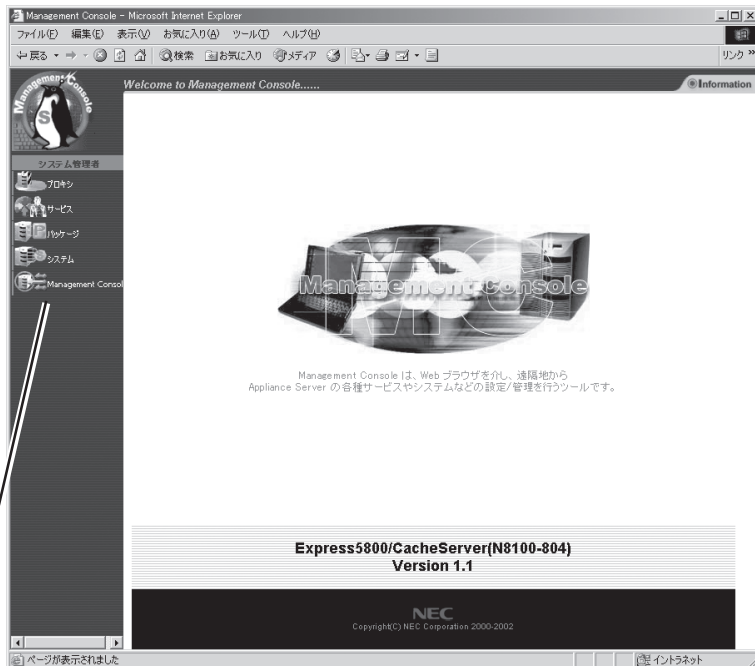
3 システムの管理

この章では、本装置で提供するサービスとWebベースの運用管理ツールである「Management Console」を利用した設定/管理について説明します。この「Management Console」からインターネットサービスに必要となるプロキシサーバを容易に管理することができます。

Management Consoleについて

ネットワーク上のクライアントマシンからWebブラウザを介して表示されるのが「Management Console」です。Management Consoleからシステムのさまざまな設定の変更や状態の確認ができます。

この章では、「管理者用」のManagement Consoleで利用できるさまざまなサービスの設定や確認、システムの操作方法を中心に説明します。

Management Console管理者用トップページ

ブラウザ上から項目(アイコン)をクリックすると、それぞれの設定画面に移動することができる。

【Management Consoleの画面構成】

■ システム管理者用トップページ

- プロキシ
- サービス
- パッケージ
- システム
- Management Console*

* 本書では説明していません。Management Consoleのオンラインヘルプを参照して操作してください。

Management Consoleのセキュリティモード

Management Consoleでは、日常的な運用管理のセキュリティを確保するためManagement Consoleに2つのセキュリティモードをサポートしています。

- **レベル1（パスワード）**

  パスワード認証による利用者チェックを行います。ただし、パスワードや設定情報は暗号化されません。

- **レベル2（パスワード + SSL）**

  パスワード認証に加えて、パスワードや設定情報をSSL（Secure Soket layer）で暗号化して送受信します。自己署名証明書を用いていますので、ブラウザでアクセスする際に警告ダイアログボックスが表示されますが、[はい]ボタンなどをクリックしてください。

デフォルトの設定では、「レベル1」に設定されています。セキュリティレベルを変更する場合は、Management Console画面の [Management Console]アイコンをクリックして設定を変更してください。また、同画面で操作可能ホストを設定することにより、さらに高いレベルのセキュリティを保つことができます。

Management Consoleへのアクセス方法

システム管理者は、Management Consoleを利用することにより、クライアント側のブラウザからネットワークを介してあらゆるサービスを簡単な操作で一元的に管理することができます。以下に各セキュリティモードにおけるアクセス手順を示します。

重要

- **Management Consoleへのアクセスには、プロキシを経由させないでください。**
- **インターネット側からManagement Consoleにアクセスする場合は、レベル2に設定してください。**
- **レベル2では、HTTPSプロトコル、ポート番号50443を使用します。**
- **Management Consoleへアクセスする場合にはブラウザのキャッシュ機能を使用しないようにしてください。**

レベル1の場合

1. クライアント側のブラウザを起動する。
2. URL入力欄に「http://<本装置に割り当てたIPアドレスまたはFQDN>:50080/」と入力する。
3. 「Management Console」画面で、[管理者用]をクリックする。
4. ユーザー名とパスワードの入力を要求されたら、ユーザー名には「admin」、パスワードにはセットアップ時に指定した管理者パスワードを入力する。

レベル2の場合

1. クライアント側のブラウザを起動する。
2. URL入力欄に「https://<本装置に割り当てたIPアドレスまたはFQDN>:50443/」と入力する。
3. 警告ダイアログボックスが表示されたら、[はい]ボタンなどをクリックして進む。
4. [Management Console]画面で、[管理者用]をクリックする。
5. ユーザー名とパスワードの入力を要求されたら、ユーザー名には「admin」、パスワードにはセットアップ時に指定した管理者パスワードを入力する。

Management Consoleにログインできたら、Management Console管理者用のトップページが表示されます。

プロキシ

頻繁にアクセスするページをキャッシング(プロキシサーバのディスクにコピーを保持しておく)ことにより、次回、同じページにアクセスした際に、ブラウザの表示時間を短縮します。
システムの管理者は、Management Consoleから、有害なWebサイトなどへのアクセスの制限、不正なアクセスの制限などを設定することができます。
また、頻繁に参照されるWebページを本装置に自動的にダウンロードさせ、本装置に格納しておくための設定もできます。
これらの設定により、効率的なインターネットへのアクセスを実現します。

【プロキシサーバの状態】

- プロキシサーバの状態表示

  プロキシサーバの起動状態を表示します。

- スケジュールダウンロード の状態表示、および一時停止/再開設定

  コンテンツを定期的にダウンロードしてキャッシュに格納するスケジュールダウンロードの状態を表示します。スケジュールダウンロードの使用を止める場合には、[停止]ボタンをクリックしてください。スケジュールダウンロードの再開は[起動]ボタンをクリックします。

【プロキシサーバの設定】

- 基本設定

  ブラウザからの要求を受け付けるIPアドレスやポート番号など、プロキシを動作させるための基本的な設定をサーバ種別に応じて設定します。

- 親プロキシ設定

  親プロキシの指定と、親プロキシの選択方法を設定します。

- 隣接プロキシ

  隣接プロキシを指定し、隣接プロキシの問い合わせ方法の設定をします。

- 詳細設定

  最大キャッシュサイズなどの詳細な設定をします。

- アクセス制御

  アクセス制御に関する設定をします。

- スケジュールダウンロード

  頻繁に参照されるページをあらかじめ指定時刻にダウンロードし、キャッシュに入れておくための設定をします。

- 認証設定

  LdapやRadiusサーバに対する認証のための設定をします。

【フィルター設定】

- フィルター選択

  使用するフィルタリングソフトを選択します。選択されたフィルタリングソフトに応じて次の設定画面へのリンクが表示されます。

- SmartFilter設定

  SmartFilterを使用するための設定をします。

- Interscan設定

  Interscanを使用するための設定をします。

プロキシサーバの設定

[プロキシ]画面の[プロキシサーバの設定]で設定できる項目について説明します。

基本設定(フォワードプロキシ)

[プロキシ]画面の[基本設定]でプロキシサーバの基本的な動作設定ができます。[基本設定]画面では、以下の項目の設定ができます。

■ サーバ種別

プロキシサーバの動作種別を、[フォワード]、[フォワード(透過型L4スイッチ)]、[フォワード(透過型WCCP)]、[リバース]の4つから選択します。

- サーバ種別を変更するとアクセス制御のプロキシ転送設定が消去されます。
- [リバース]を選択した場合は、リバースプロキシの設定ページが表示されます。

■ キャッシュサーバ設定

キャッシュサーバのIPアドレスと、HTTPの要求を受け付けるポート番号を指定します。登録されているIPアドレスとポート番号の組は、リストボックスに表示されます。
[追加]、[編集]、[削除]ボタンで、設定を行います。

- 登録できるIPアドレスとポート番号の組は最大16個です。
- [キャッシュサーバIPアドレス]で選択できるIPアドレスは、[システム]－[簡易ルータ設定]画面で登録したIPアドレスのみが表示されます。

■ ICPポート番号設定

本装置がICP要求を受け付けるポート番号を指定します。通常は3130を指定します。ICP要求を受け付けたくない場合には「ICP要求を受け付けない」を指定してください。

■ WCCP設定

ルータアドレスで、WCCPルータのIPアドレスを指定します。登録されているWCCPルータのIPアドレスはリストボックスに表示されます。[追加]、[編集]、[削除]ボタンで設定します。

- キャッシュサーバIPアドレス

  WCCPルータからパケットを転送するキャッシュサーバのIPアドレスを指定します。

- バージョン

  WCCPのバージョンを指定します。指定できるバージョンは[1]か[2]です。

- マルチキャストIP

  WCCPルータがマルチキャストIPを使用するかどうかを指定します。指定できるIPアドレスの範囲は、224.0.0.0-239.255.255.255になります。マルチキャストIP使用時はルータアドレスの設定は無効になります。

- パスワード

  認証を行うためのパスワードを指定します。

- HASH方法

  HASH方法を指定します。

重要

- WCCP設定は、サーバ種別で[フォワード(透過型WCCP)]を選択した時のみ有効になります。
- [設定]ボタンをクリックしないと、システムに反映されません。
- 設定項目の詳細は、[ヘルプ]をクリックし、オンラインヘルプを参照してください。

基本設定(リバースプロキシ)

[プロキシ]画面の[基本設定]でサーバ種別設定を「リバース」と選ぶことによって表示される画面です。この画面では、本装置をリバースモードで運用する際の設定ができます(CacheServerをリバースモードで運用するにはDNSサーバとの連携が必須です)。

■ サーバ種別設定

リバースモードで動作するため、「リバース」と言う文字が表示されています。

■ サーバの持続性

複数Webサーバの負荷を軽減するため本装置を導入する場合、クライアントIPアドレスによって接続するWebサーバを一意に限定したい場合に有効にしてください。このチェックをONにすることによりクライアントは複数あるWebサーバの内常に特定のWebサーバにアクセスすることができます(注:本装置に直接接続してきているクライアントのIPアドレスによって持続性を確保しているため、接続ルートが異なると持続性が確保されません)。

■ DNS名チェック

本装置が受け付けた要求に示されているWebサーバのホスト名と[DNS設定]で設定したDNS名(ホスト名)が同一となっているかチェックしたい場合に有効にしてください。有効にした場合にどのDNS名とも同一でないホスト名の要求は拒否されます。

重要

HTTPSの場合はチェックされません。

■ キャッシュサーバ設定

本装置のHTTP要求を受け付けるIPアドレスとポート番号を設定します。登録できるIPアドレスとポート番号の組は最大16個です。ポート番号は80,443,1025〜65535を指定できます。

■ DNS設定

Internetに公開するWebサーバのホスト名を設定してください。また、本装置は1つのIPアドレスに対して複数のホスト名を持つことができます。別々のコンテンツを持つ2つのWebサーバのホスト名を本装置のIPアドレスに解決されるようにDNSサーバに設定してください。本装置は ホスト名を見分けて別々に処理することができます。本装置は1つのキャッシュサーバ設定に対して16個のホスト名を設定できます。

■ Webサーバ設定

実際のWebサーバのIPアドレスとポート番号を指定してください。また、本装置は 1つのDNS名に対して複数のWebサーバを設定できます(このような構成とした場合 設定された複数のWebサーバは同一のコンテンツを提供する必要があります)。本装置は1つのDNS名に対して16個のWebサーバを設定することができます。

重要

- キャッシュサーバを登録、変更する場合には 必ず、[追加]、[編集]ボタンをクリックしてください。DNS設定やWebサーバ設定についても同様です。
- [設定]ボタンをクリックしないと、システムに反映されません。
- ReverseHTTPSとして運用される場合には、DNS名を1つだけ設定してください。
- HTTPSのポート番号は、443で固定です。
- リバースプロキシが対応するプロトコルは HTTPとHTTPSです。

親プロキシ設定

階層構造を形成する場合に本装置の親プロキシサーバを設定することができます。

- **ホスト名**

  親プロキシのホスト名またはIPアドレスを設定してください。隣接プロキシに設定してあるホスト名およびIPアドレスは指定できません。255文字まで指定できます。

- **HTTPポート番号**

  親プロキシのHTTP要求待ち受けポート番号を指定してください。

- **連携サーバのコンテンツをキャッシュ**

  親サーバを経由して取得したコンテンツをキャッシュしてほしくない場合に「しない」を設定してください。

- **ユーザー名/パスワード/パスワード確認**

  親プロキシが認証機能を有している場合、ユーザー名、パスワードの指定を行います。親プロキシが認証を必要とする場合はユーザー名、パスワードの指定は必須です。親プロキシに接続する際に指定したユーザー名とパスワードでアクセスします。親プロキシが認証を必要としない場合は、設定する必要はありません。

- **プロキシ選択方式**

  複数の親プロキシを設定した場合に、その中からどの親プロキシを選ぶかといった選択方式を設定できます。

  - アクセス制御を使用

    条件式を満たした場合に現在選択されている親プロキシに接続する方式(条件式の具体例はManagemant Consoleのヘルプを参照してください)。

  - ROUND-ROBINを使用

    複数の親プロキシを順番に選択する方式です。その際、現在選択されている親プロキシが選択される頻度を重み付けとして設定できます(数字が大きいほど頻度が高くなります)。

  - RESP-TIMEを使用

    応答速度の速い親プロキシが優先的に選択される方式。

  - CARPを使用

    URLごとに接続先の親プロキシを一意に選択するプロトコル「CARP」を利用する方式。 現在選択されている親プロキシが選択される割合を指定できます(割合の合計が1.0になるように設定してください)。

  - 問い合わせなし

    親プロキシが単一の場合はこの設定にしてください。

親プロキシの選択方法にアクセス制御を使用を選んだ場合、条件式は、親サーバの順にチェックされます。[順序]ボタンをクリックして適した順番に変更することができます。

- **親プロキシを登録、変更する場合には必ず、[追加]または[編集]ボタンをクリックしてください。DNS設定やWebサーバ設定についても同様です。**
- **[設定]ボタンをクリックしないと、システムに反映されません。**

隣接プロキシ設定

階層構造を形成する場合にCacheServerの隣接プロキシサーバを設定することができます。

- **ホスト名**

  隣接プロキシのホスト名またはIPアドレスを設定してください。親プロキシに設定してあるホスト名およびIPアドレスは指定できません。255文字まで指定できます。

- **HTTPポート番号**

  隣接プロキシのHTTP要求待ち受けポート番号を指定してください。

- **ICPポート番号**

  隣接サーバのICP要求待ち受けポートを指定してください。本装置は隣接サーバと連携する際にICPを利用します。

- **連携サーバのコンテンツをキャッシュ**

  隣接サーバを経由して取得したコンテンツをキャッシュしたくない場合に「しない」を選択してください。

- **ユーザー名/パスワード/パスワード確認**

  隣接プロキシが認証機能を有している場合、ユーザー名、パスワードの指定を行います。連携プロキシが認証を必要とする場合はユーザー名、パスワードの指定は必須です。隣接プロキシに接続する際にこのユーザー名とパスワードでアクセスします。隣接プロキシが認証を必要としない場合は、設定する必要はありません。

重要

- **本装置がICPサーバとして動作する場合、本装置のIPアドレスは一種類となります(複数に対応していません)。隣接プロキシ側に設定する本装置のIPアドレスはシステムの簡易ルータ設定で一番上に登録したIPアドレスを適用してください。**
- **隣接プロキシを設定すると、指定した隣接サーバの設定によっては、web閲覧の際にページや画像が正しく表示されない場合があります。**

  指定した隣接サーバの設定を確認し、設定し直すか、ここでの設定を削除してください(7章の「トラブルシューティング」も併せて参照してください)。

詳細設定

[プロキシ]画面の[詳細設定]でプロキシサーバとしての詳細な動作設定ができます。
[詳細設定]画面では、以下の項目の設定ができます。

■ 詳細設定

項目	設定値
最大キャッシュサイズ	16 MB
Webサーバ接続最大待ち時間	120 秒
Read要求最大待ち時間	15 分
クライアント接続維持時間	300 秒
最大クライアント接続維持時間	1 日
クライアントIPの通知	しない
リクエストボディサイズの上限値	1 MB
レスポンスサイズの上限値	0 KB
DNSリトライ間隔	3 秒
DNSリトライ数	4 回
FTPのPASVモード	有効にする
FTPのパスワード	guest@
Viaヘッダ	1.1 NEC-Cache
デフォルト値に戻す	

設定　戻る

- **最大キャッシュサイズ**

  この設定サイズよりも大きなデータはディスクに保存されません。0KB～999MBまで指定できます。0が指定されると制限無しとなります。デフォルトは[16MB]です。

- **Webサーバ接続最大待ち時間**

  Webサーバへの接続タイムアウト時間を指定します。30秒～99日まで指定できます。デフォルトは[120秒]です。

- **Read要求最大待ち時間**

  Webサーバへの要求に対して応答待ちをする時間を指定します。30秒～99日まで指定できます。デフォルトは[15分]です。

- **クライアント接続維持時間**

  クライアントからの接続を維持する最大無応答時間を指定します。30秒～99日まで指定可能です。デフォルトは[300秒]です。

- **最大クライアント接続維持時間**

  クライアントからの接続を維持する最大時間を指定します。30秒～99日まで指定できます。デフォルトは[1日]です。

- **クライアントIPの通知**

  要求してきたクライアントのIPアドレスをヘッダ情報としてWebサーバに通知するかどうかを指定します。デフォルトは[しない]です。

- **リクエストボディサイズの上限値**

  クライアントからのリクエストボディサイズの上限値を指定します。0KB～999MBまで指定できます。0が指定されると制限無しとなります。デフォルトは[1MB]です。

- **レスポンスサイズの上限値**

  Webサーバからのレスポンスサイズの上限値を指定します。0KB～999MBまで指定できます。0が指定されると制限無しとなります。デフォルトは[0(無制限)]です。

- **DNSリトライ間隔**

  DNSサーバへのリトライ間隔を指定します。1秒～99秒まで指定できます。デフォルトは[3秒]です。

● DNSリトライ数

DNSサーバへのリトライ回数を指定します。1回〜99回まで指定できます。デフォルトは[4回]です。

● FTPのパスワード

anonymous FTP サーバへ接続する場合に、パスワード情報として送信される文字列を指定します。通常はメールアドレスを指定することが多いですが、この情報はFTPサーバに送信されるため慎重に設定してください。 デフォルトは[guest@]です。

● Viaヘッダ

HTTPのViaヘッダを指定します。255文字まで設定可能です。指定されたヘッダの先頭には必ず「1.1 」が付きます。デフォルトは「1.1 ホスト名」です。Viaヘッダは英数字と「ー」を指定することができます。

重要

- **[デフォルト値に戻す]ボタンをクリックすると、すべての設定項目をデフォルト値に戻すことができます。**
- **[設定]ボタンをクリックしないと、システムに反映されません。[デフォルト値に戻す]を行った場合も、[設定]ボタンをクリックして必ず反映してください。**
- **設定項目の詳細については、[ヘルプ]をクリックし、オンラインヘルプを参照してください。**

DNSサーバの設定変更は[ヘルプ]をクリックし、オンラインヘルプを参照してください。

アクセス制御設定

[プロキシ]画面の[アクセス制御設定]ではプロキシサーバを通じてアクセス許可/禁止や、キャッシュ許可/禁止、プロキシの使用許可/禁止とする条件が登録できます。アクセス制御は、最初に条件を持つリストを登録し、それぞれのリストに対しての動作条件(アクセス制御、非キャッシュ設定、プロキシ転送)を設定していくという流れになります。デフォルトは、リスト設定に「リスト名:all , 設定種別:src , 条件式 0.0.0.0/0.0.0.0」、「リスト名:cgi , 設定種別:url_pathregex , 条件式 .cgi$ ¥?」、アクセス制御設定に「allow/deny:allow , all」、非キャッシュ設定に「allow/deny: deny , cgi」です。

- アクセス制御設定において、リストをまったく設定しない場合、または指定した条件のいずれにも該当しないアクセス要求は、「アクセスを許可する」として扱われます。
- アクセス制御設定、非キャッシュ設定、プロキシ転送設定合わせて最大100個まで設定することが可能です。

リスト設定

- **リストの追加**

リストを登録するには、アクセス制御の上画面に表示されている[リスト設定]画面から、[追加]ボタンをクリックします。

- [追加]ボタンをクリックすることで、[リスト(追加)設定]画面を開くことができます。
- [リスト(追加)設定]画面で入力できるリスト名は、半角英数字16文字(先頭に数字は不可)以内です。

- [設定]ボタンをクリックしないと、システムに反映されません。
- 設定種別や条件式の詳細については、[ヘルプ]をクリックし、オンラインヘルプを参照してください。

● リストの編集

リストを編集するには、アクセス制御の上画面に表示されている[リスト設定]画面から編集したいリスト名の左横にある[編集]ボタンをクリックします。

- [編集]ボタンをクリックすることで、[リスト(編集)設定]画面を開くことができます。
- [リスト(編集)設定]画面には、選択したリストの情報が表示されます。

- **[設定]ボタンをクリックしないと、システムに反映されません。**
- **設定項目の詳細については、[ヘルプ]をクリックし、オンラインヘルプを参照してください。**

● リストの削除

リストを削除するには、アクセス制御の上画面に表示されている[リスト設定]画面から削除したいリスト名の左横にある[削除]ボタンをクリックします。画面に削除するかどうかの確認を求めるダイアログボックスが表示されます。削除する場合は、[OK]ボタンをクリックしてください。

動作条件の設定

アクセス制御の下の画面では、登録したリストに対して動作条件の設定を行います。3つの動作について設定することができます。

● **アクセス制御設定**

登録したリストに対して、アクセスの許可(禁止)を設定します。

追加 順序	allow/deny	リスト名
編集 削除	deny	Method1
編集 削除	deny	xxxxxxxxxxxxxx

ー　アクセス制御の追加

アクセス制御リストを追加をするには、アクセス制御設定の[追加]ボタンをクリックします。

- [追加]ボタンをクリックすることで、[アクセス制御(追加)設定]画面を開くことができます。
- アクセス制御したいリストを選択し、アクセスの許可(allow)か禁止(deny)かを決定します。
- リストは複数選択することができます。
- リストを複数指定した場合にはANDの処理が行われます。

- **[設定]ボタンをクリックしないと、システムに反映されません。**
- **設定項目の詳細については、[ヘルプ]をクリックし、オンラインヘルプを参照してください。**

― アクセス制御の編集

アクセス制御リストを編集するには、編集したいリスト名の左横にある[編集]ボタンをクリックします。

■アクセス制御(編集)設定

allow/deny ◉ allow ○ deny

アクセス制御リスト

※指定したリスト名を含みます

xxxxxxxxxxxxx
Method1

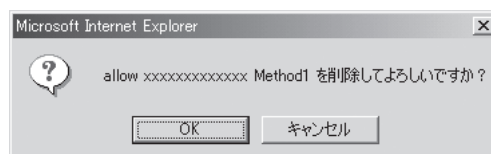
設定　戻る

- [編集]ボタンをクリックすることで、[アクセス制御(編集)設定]画面を開くことができます。
- [アクセス制御(編集)設定]画面には、選択したリストの情報が表示されます。
- リストを複数指定した場合にはANDの処理が行われます。

重要

- **[設定]ボタンをクリックしないと、システムに反映されません。**
- **設定項目の詳細については、[ヘルプ]をクリックし、オンラインヘルプを参照してください。**

― アクセス制御の削除

アクセス制御リストを削除するには、削除したいリスト名の左横にある[削除]ボタンをクリックします。画面に削除するかどうかの確認を求めるダイアログボックスが表示されます。削除する場合は、[OK]ボタンをクリックしてください。

― 順序の設定

アクセス制御の順序を設定することができます。[順序]ボタンをクリックすると、順序設定画面が表示されます。優先度を変更したいリストを選択し、[UP]か[DOWN]ボタンをクリックすることで設定することができます。

重要

- **順序は一番上が優先度が高く、下になるにつれて優先度が低くなります。**
- **[実行]ボタンをクリックしないと、システムに反映されません。**

● 非キャッシュ設定

登録したリストに対して、キャッシュしてもよい(してはいけない)を設定します。

非キャッシュ設定		
追加 順序	allow/deny	リスト名
編集 削除	allow	Method1

ー 非キャッシュ設定の追加

非キャッシュ設定リストを追加をするには、非キャッシュ設定の[追加]ボタンをクリックします。

- [追加]ボタンをクリックすることで、[非キャッシュ(追加)設定]画面を開くことができます。
- キャッシュ制御したいリストを選択し、アクセスの許可(allow)か禁止(deny)かを決定します。
- リストは複数選択することができます。
- リストを複数指定した場合にはANDの処理が行われます。

重要

- **[設定]ボタンをクリックしないと、システムに反映されません。**
- **設定項目の詳細については、[ヘルプ]をクリックし、オンラインヘルプを参照してください。**

ー 非キャッシュ設定の編集

非キャッシュ設定リストを編集するには、編集したいリスト名の左横にある[編集]ボタンをクリックします。

- **[編集]ボタンをクリックすることで、[非キャッシュ(編集)設定]画面を開くことができます。**
- **[非キャッシュ設定(編集)設定]画面には、選択したリストの情報が表示されます。**
- **リストを複数指定した場合にはANDの処理が行われます。**

重要

- **[設定]ボタンをクリックしないと、システムに反映されません。**
- **設定項目の詳細については、[ヘルプ]をクリックし、オンラインヘルプを参照してください。**

－　非キャッシュ設定の削除

非キャッシュ設定リストを削除するには、削除したいリスト名の左横にある[削除]ボタンをクリックします。画面に削除するかどうかの確認を求めるダイアログボックスが表示されます。 削除する場合は、[OK]ボタンをクリックしてください。

－　順序の設定

非キャッシュ設定の順序を設定することができます。[順序]ボタンをクリックすると、順序設定画面が表示されます。優先度を変更したいリストを選択し、[UP]か[DOWN]ボタンをクリックすることで設定することができます。

- **順序は一番上が優先度が高く、下に行くにつれて優先度が低くなります。**
- **[実行]ボタンをクリックしないと、システムに反映されません。**

● **プロキシ転送設定**

登録したリストに対して、隣接プロキシを使用する(使用しない)を設定します。

プロキシ転送設定

		転送種別	allow/deny	リスト名
追加	順序			
編集	削除	Always_direct	allow	xxxxxxxxxxxxx

－　プロキシ転送設定の追加

プロキシ転送設定リストを追加するには、追加したいリスト名の左横にある[追加]ボタンをクリックします。

- [追加]ボタンをクリックすることで、[プロキシ転送(追加)設定]画面を開くことができます。
- 常にWebサーバへの接続をプロシキ経由で転送する(Never_direct)か、常に直接Webサーバへ接続する(Always_direct)を[転送種別]から選択します。
- それぞれの設定に対して、許可する(allow)、許可しない(deny)を設定します。
- リストを複数選択した場合にはANDの処理が行われます。

重要

- **[設定]ボタンをクリックしないと、システムに反映されません。**
- **設定項目の詳細については、[ヘルプ]をクリックし、オンラインヘルプを参照してください。**

ー　プロキシ転送設定の編集

プロキシ転送設定リストを追加をするには、プロキシ転送設定の[編集]ボタンをクリックします。

- [編集]ボタンをクリックすることで、[プロキシ転送(編集)設定]画面を開くことができます。
- [プロキシ転送設定(編集)設定]画面には、選択したリストの情報が表示されます。
- リストを複数指定した場合にはANDの処理が行われます。

重要

- **[設定]ボタンをクリックしないと、システムに反映されません。**
- **設定項目の詳細については、[ヘルプ]をクリックし、オンラインヘルプを参照してください。**

ー　プロキシ転送設定の削除

プロキシ転送設定リストを削除するには、削除したいリスト名の左横にある[削除]ボタンをクリックします。画面に削除するかどうかの確認を求めるダイアログボックスが表示されます。削除する場合は、[OK]ボタンをクリックしてください。

ー　順序の設定

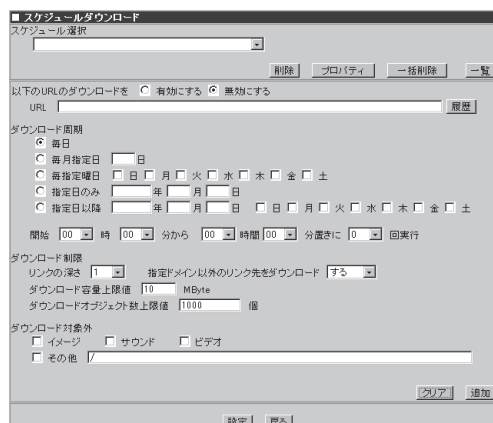
プロキシ転送設定の順序を設定することができます。[順序]ボタンをクリックすると、順序設定画面が表示されます。優先度を変更したいリストを選択し、[UP]か[DOWN]ボタンをクリックすることで設定することができます。

- **順序は一番上が優先度が高く、下になるにつれて優先度が低くなります。**
- **[実行]ボタンをクリックしないと、システムに反映されません。**

スケジュールダウンロード

スケジュールダウンロードとは、頻繁に参照されるページをあらかじめ指定時刻にダウンロードし、キャッシュに入れておく機能です。
対象となるURL、ダウンロード周期などスケジュールダウンロードの設定ができます。

重要

コンテンツの性質とサイズによってはキャッシュされないこともあります。

スケジュールの新規追加

スケジュールを追加するには、対象となるURL、ダウンロード周期などを設定し[追加]ボタンをクリックします。スケジュールは最大100件まで追加できます。
下に示す図と手順の流れの関係は次のとおりです。

① 「有効にする」を選択する。

② ダウンロードするＵＲＬを入力する（例：http://www.nec8.com/）。

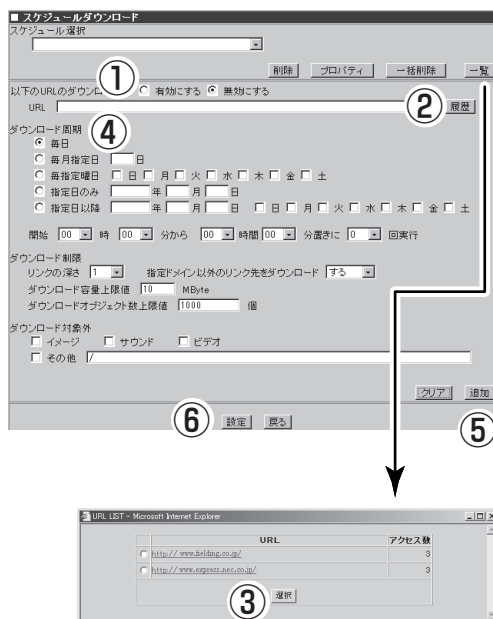
③ ＜履歴＞ボタンをクリックする。

[URL LIST]画面が表示されます。

④ ダウンロード周期、ダウンロード制限、ダウンロード対象外の項目を必要に応じて設定する。

各項目の詳細はManagement Consoleのヘルプを参照してください。

⑤ ＜追加＞ボタンをクリックしてダウンロードしたいURLを追加する。

⑥ ＜設定＞ボタンをクリックする。

- **設定項目の詳細については、[ヘルプ]をクリックしてオンラインヘルプを参照してください。**
- **履歴機能が有効になるのは、[システム]画面の[プロキシアクセス統計]でプロキシアクセス統計を「有効にする」を設定した時だけです。**

スケジュールの変更

スケジュールを変更するには、[スケジュール選択]欄からスケジュールを選択し、変更したい項目を編集します。

引き続き別のスケジュールを編集するときは、そのまま一覧から選択してください。編集内容はウィンドウ内で一時保存されます。

重要

- **[設定]ボタンをクリックしないと、システムに反映されません。**
- **設定項目の詳細については、[ヘルプ]をクリックし、オンラインヘルプを参照してください。**

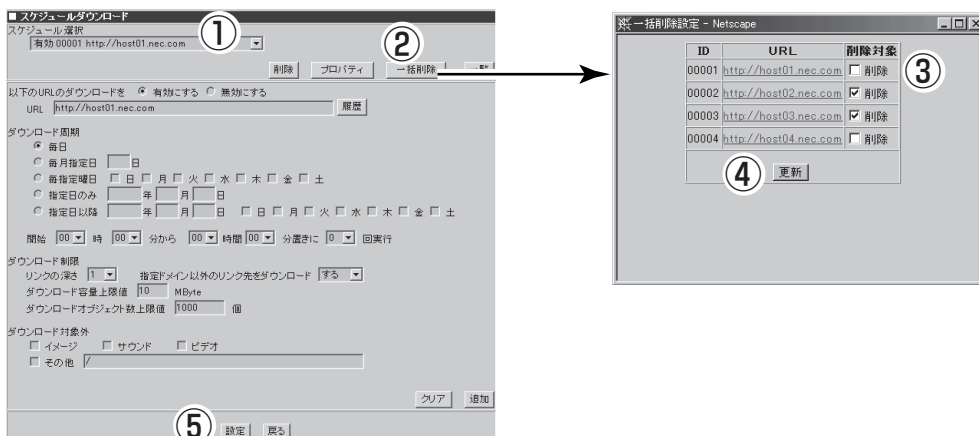
スケジュールの削除

スケジュールを削除するには、[スケジュール選択]欄からスケジュールを選択し、[削除]ボタンをクリックします。

[設定]ボタンをクリックしないと、システムに反映されません。

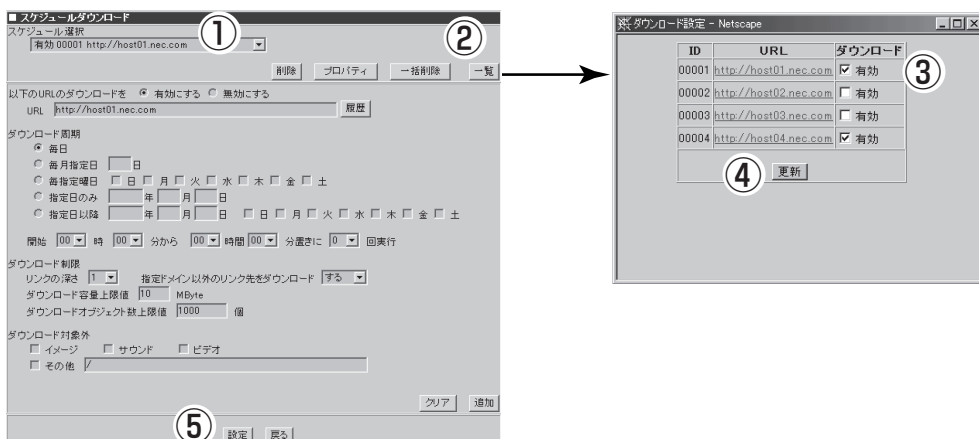
スケジュールの一括削除

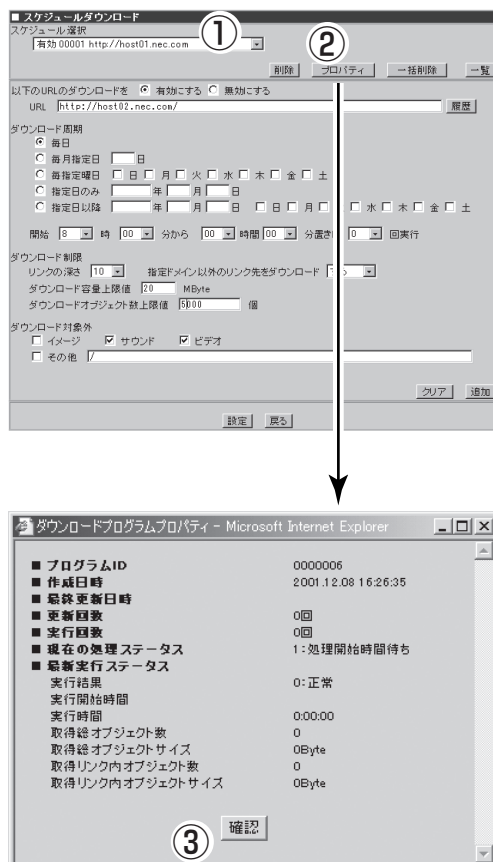
[一括削除]ボタンをクリックすることで[一括削除設定]画面を開くことができます。
[一括削除設定]画面で、削除したいスケジュールの[削除対象]をチェックし[更新]ボタンをクリックすると、[スケジュール選択]欄から削除されます。

[設定]ボタンをクリックしないと、システムに反映されません。

スケジュールの一括設定

[一覧]ボタンをクリックすることで[ダウンロード設定]画面を開くことができます。
[ダウンロード設定]画面で、ダウンロードを実行したいスケジュールの[ダウンロード]をチェックし[更新]ボタンをクリックすると、[スケジュール選択]欄に反映されます。

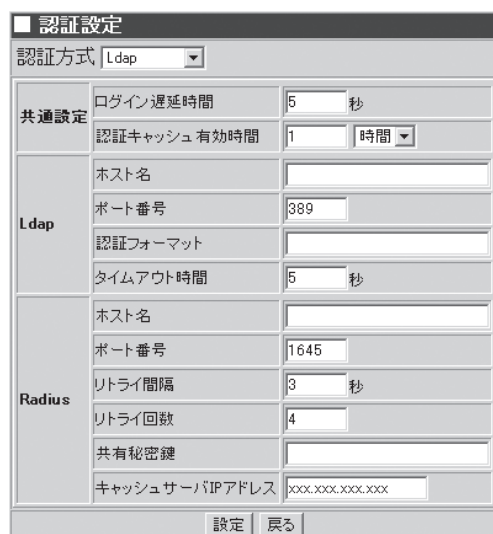
ダウンロードを実行する時は[ダウンロード]にチェックを付け、実行しない時はチェックを外してください。

[設定]ボタンをクリックしないと、システムに反映されません。

スケジュールの確認

[プロパティ]ボタンをクリックすると、選択したスケジュールの設定履歴や最新のダウンロード結果などを表示します。

認証設定

[プロキシ]画面の[認証設定]で、キャッシュサーバを使用するユーザーを認証するための設定ができます。[認証設定]画面では、以下の項目を設定することができます。

● **認証方式**

ユーザー認証を行うために使用する方式を指定します。[Ldap]と[Radius]から選択することが可能です。ユーザー認証を行わない場合は、[認証しない]を指定してください。

- **共通設定**
  - ログイン遅延時間

    LdapサーバやRadiusサーバへのログイン時にエラーが発生した場合の遅延時間を指定します。
  - 認証キャッシュ有効時間

    パスワードをキャッシュサーバが保持している時間を設定します。 1分から99時間まで指定可能です。デフォルトは1時間です。
- Ldap
  - ホスト名

    Ldapサーバのホスト名(IPアドレスも可)を指定します。
  - ポート番号

    Ldapサーバとの接続に使用するポート番号を指定します。通常は389を指定します。
  - 認証フォーマット

    Ldapで認証を行う際、ユーザー名からDN(Distinguished Name)と呼ばれる識別名に変換するためのフォーマットを指定します。
  - タイムアウト時間

    Ldapサーバとの通信タイムアウト時間を指定します。デフォルトは[60秒]です。

- Radius
  - ホスト名

    Radiusサーバのホスト名(IPアドレスも可)を指定します。
  - ポート番号

    Radiusサーバとの接続に使用するポート番号を指定します。通常は1645を指定します。
  - リトライ間隔

    Radiusサーバへのリトライ間隔を指定します。デフォルトは[3秒]です。
  - リトライ回数

    Radiusサーバへのリトライ回数を指定します。デフォルトは[4回]です。
  - 共有秘密鍵

    Radiusサーバと共有する秘密鍵を指定します。Radiusはこの秘密鍵を使って、認証応答用の識別子を生成します。
  - キャッシュサーバIPアドレス

    Radiusサーバと通信を行うためのキャッシュサーバのIPアドレスを指定します。キャッシュサーバが複数のIPアドレスをサポートしている場合は、その中の1つを指定します。1つのIPアドレスしかサポートしていない場合は、そのIPアドレスを指定します。

- ［設定］ボタンをクリックしないと、本装置に反映されませんので注意してください。
- 設定項目の詳細については、［ヘルプ］をクリックし、オンラインヘルプを参照してください。

バイパス設定

［プロキシ］画面の［バイパス設定］では、本装置を透過型プロキシとして動作させる際の、静的バイパス・動的バイパスの設定を行います。

■ 静的バイパス

本装置を透過型プロキシとして動作させる際に、指定したIPアドレスのWebサーバへのアクセス要求がCacheServerに来た時、本装置を経由させずに直接アクセス（バイパス）させます。

- IPアドレス

  本装置を経由させず直接アクセスさせるWebサーバのIPアドレスを指定します。

■ 動的バイパス

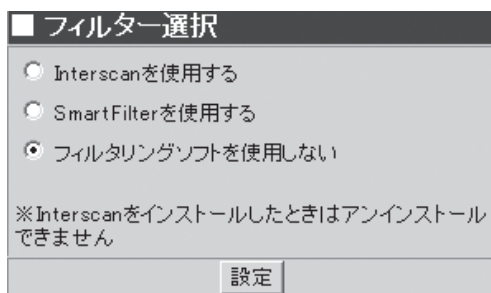
本装置を透過型として利用する際に利用できます。指定した条件のHTTP応答を本装置が受け取った場合、今後 その応答を返したWebサーバへのアクセス要求は本装置を経由させずに直接アクセス（バイパス）させます。

- HTTP応答コード検出

  HTTPの応答コードの種類でバイパスを行います。条件に加える応答コードをチェックしてください。また、表示されていないコードを加える場合は、その他欄に、コードの数値をカンマで区切って入力してください。

- HTTP以外のトラフィック検出

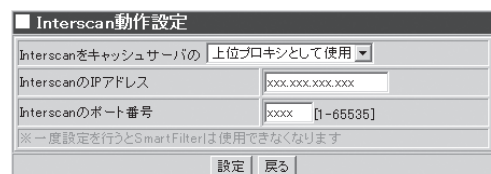
  HTTP以外のトラフィックをバイパスする場合はチェックを付けてください。

- バイパス時間

  動的にバイパスを行う時間を指定します。秒単位で指定してください。

重要

- 静的バイパスのIPアドレスを登録、変更する場合には 必ず、［追加］や［編集］ボタンをクリックしてください。
- ［設定］ボタンをクリックしないと本装置の動作に反映されませんので注意してください。
- 上記のバイパス設定は、本装置を透過型で使用した時のみ機能します。

フィルター設定

［プロキシ］画面の［フィルター選択］画面で、使用するフィルタリングソフトを選択することができます。フィルタリングソフトはInterscanとSmartFilterを使用することができます。

SmrtFilterを使用していて、フィルタリングソフトを使用しないを設定した時、SmartFilter動作設定のSmartFilterによるフィルタリングとフィルタリングデータベースの自動更新は「実行しない」が自動的に設定されます。

- **Interscanを一度インストールするとアンインストールすることはできません。**
- **SmartFilterを使用していて、Interscanを使用したくなった場合にはいったんフィルタリングソフトを使用しないを設定してからInterscanをインストールしてください。**
- **SmartFilterやInterscanWebManagerを使用する場合は512MB以上のメモリが必要です。**

システムの管理

Interscan設定

［プロキシ］画面の［フィルター選択］画面の［Interscan設定］で、Interscanの設定を行います。この設定はInterscanを本装置内で使用するとき必ず必要です。IPアドレスとポート番号の指定はInterscanWebManagerで設定する内容に従って設定してください。なお、この画面でIPアドレスとポート番号を変更してもInterscanWebManagerには反映されません。

- Interscan設定で設定を行った後、［プロキシ］画面に［Interscan設定］の項目が表示されるようになります。
- 「Interscanを上位プロキシとして使用」を設定した時、［プロキシ］画面の［アクセス制御設定］にて設定したプロキシ転送設定が削除されます。
- 「Interscanを上位プロキシとして使用」を設定した時、［プロキシ］画面の［隣接プロキシ］設定にて設定した内容が削除されます。
- 「Interscanを上位プロキシとして使用」を設定した時、［プロキシ］画面の［親プロキシ］設定にInterscanが設定され、他の親プロキシの設定は削除されます。
- 「Interscanを上位プロキシとして使用」を設定した時、［プロキシ］画面の［認証設定］の認証方式が「認証しない」に設定され、変更できなくなります。

重要

- Interscanを一度インストールするとアンインストールすることはできません。アンインストールする場合にはシステムを再インストールしてください。
- 本装置を透過型として使用する場合にはInterscanは親プロキシとしてのみ使用可能です。
- 本装置をReverseプロキシとして使用する場合にはInterscanは使用できません。
- Interscanは一度インストールするとアンインストールできません。Interscanの設定を行った後は、SmartFilterを使用することはできません。
- InterscanWebManagerでInterscanのIPアドレスやポート番号を変更した場合には必ずこの画面の設定も変更してください。
- Interscanを本装置の上位プロキシとして使用する場合、Interscanの設定を変更してもエラーページがキャッシュされているため、ブラウザに拒否画面が表示されることがあります。

Interscanインストール手順

Interscanのインストール手順を示します。

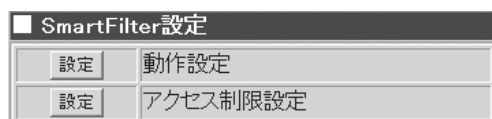
1. [システム]画面の[保守用パスワード]でmainteユーザーのパスワードを設定する。
2. [サービス]画面で「リモートログイン(TELNET)」を起動する。
3. [サービス]画面の「リモートログイン(TELNET)」をクリックして[リモートログイン(TELNET)]画面へ遷移し、本装置にリモートログインできるようにTELNETを許可するホストを設定する。
4. TELNETでmainteユーザーで本装置にリモートログインし、「su -」とコマンドラインに打ち込む。
5. パスワードを求められるので、Management Consoleにログインするためのパスワードを指定して(adminのパスワードを指定して)管理者ユーザとしてログインする。
6. Interscanのマニュアルに基づきインストールをする。Interscanインストール中にインストールディレクトリを聞かれますが、「/usr/local」を指定します。
7. Interscanインストール後、[プロキシ]画面の[フィルター選択]で「Interscanを使用する」を指定し、「設定」ボタンをクリックして表示される[Interscan設定]画面でnterscanのIPアドレスやポート番号を指定する。

SmartFilterを使用する

[プロキシ]画面の[SmartFilter設定]画面では、SmartFilterの動作設定またはアクセス制限設定の設定項目を選択します。「SmartFilter」は30種類のブロックカテゴリで、最大50万件以上のサイトへのアクセスを制限することができるフィルタリングサービスです。フィルタを設定することで無駄なトラフィックや業務に無意味なアクセス、有害なホームページへのアクセスをなくし、安心できる環境でインターネットを業務や授業に利用することができます。動作設定ではフィルタリングを実行するかどうか、データベースファイルダウンロードのための設定を行います。アクセス制限設定はどのような条件でアクセスの制限を行うかを設定します。

■ SmartFilter設定

設定	動作設定
設定	アクセス制限設定

重要

SmartFilterの機能は本装置にインストールされています。契約を行うことですぐに利用可能となります。

SmartFilter動作設定

SmartFilterの動作設定やSmartFilterを動かすために必要なactivation keyおよびデータベースファイルのダウンロード設定を行います。SmartFilterによるフィルタリングは、SmartFilterを利用したアクセス先URLのフィルタリングを実行するかどうかの設定です。activation keyは代理店より入手したactivation keyを設定します。フィルタリングデーターベースの自動更新は、週に1回更新されるSmartFilterのフィルタリングデータベースを、定期的にダウンロードするかどうかの設定です。なお、フィルタリングデータベースはFTPサイトからダウンロードされるため、ユーザー名/パスワード、FTPサイト名などの設定も必要となります。

設定項目「SmartFilterによるフィルタリング」で「実行する」を設定することで[プロキシ]画面[SmartFilter設定]の項目が表示されるようになります。

- [設定]ボタンをクリックしないと、本装置に反映されません。
- 設定項目の詳細についてはオンラインヘルプを参照してください。
- FTPサイトのホスト名、FTPサイトのパス、ファイル名はSmartFilterのバージョンによって異なります。 販売店より入手した情報を入力してください。
- データベースファイルのダウンロードをプロキシ経由で実行する場合、そのプロキシサーバはFTPプロキシに対応している必要があります。
- SmartFilterを利用する場合は、最初に必ずフィルタリングデータベースからダウンロードしてください。

SmartFilterアクセス制限設定

アクセス制限の設定をポリシーとして登録し、各クライアントについてアクセスの許可/禁止をポリシーを用いて設定を行います。ポリシー設定はポリシー名を設定し、ポリシーに対してどのカテゴリをどの時間に制限するかを設定します。クライアント設定はクライアントのIPアドレスを指定し、指定したIPに対してどのポリシーを割り当てるかを設定します。

- [追加]ボタンをクリックすることでそれぞれの[追加]画面を開くことができます。
- [編集]ボタンをクリックすることで、設定されているポリシー、クライアント設定を編集することができます。
- [削除]ボタンをクリックすることで、設定されているポリシー、クライアント設定を削除することができます。

- **クライアント設定で設定していないクライアントは接続を拒否されます。**
- **異なる複数のアクセスが同じIPに割り当てられると正しくフィルタリングされません。**

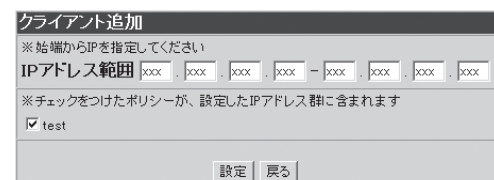
- **ポリシー設定(ポリシー追加/編集)**

ポリシー名とアクセスの設定を行います。ポリシー名は英数字のみ設定可能です。アクセスは全て許可、全て拒否、カスタムの中から一つ選択します。アクセスを「全て許可」を設定した時、全カテゴリをすべての時間でアクセスを許可することとなります。アクセスを「全て拒否」を設定した時、全カテゴリをすべての時間でアクセスを拒否することとなります。カスタムは時間別、カテゴリ別にアクセスの許可、拒否を設定することができます。

カスタムを設定した時、[ポリシーカスタム設定]画面を開くことができます。

作成したポリシー名がすでに存在していたとき、ポリシーの追加(編集)を行うことはできません。

● **ポリシーカスタム設定**

カスタムは時間別、カテゴリ別にアクセスの許可、拒否を設定することができます。カテゴリ選択ではカテゴリの一覧からカテゴリを選択します。 選択したカテゴリのアクセス制限状況がカスタム設定の中央詳細部に表示されます。なお、カテゴリについての詳細は、オンラインヘルプの[SmartFilterの概要]画面にて参照してください。カスタム設定ではカテゴリ欄で選択したカテゴリに対するアクセスの許可/拒否を曜日、時間別に指定します。

- カスタム設定の [全て許可]ボタンをクリックすることで、カテゴリ選択で選択したカテゴリに対し、全ての時間アクセスを許可する設定を行うことができます。
- カスタム設定の[全て拒否]ボタンをクリックすることで、カテゴリ選択で選択したカテゴリに対し、全ての時間アクセスを拒否する設定を行うことができます。
- カスタム設定下部で曜日、時間別に詳細な設定を行うことができます。

重要

[全て許可]、[全て拒否]、[設定]ボタンをクリックすることで設定が直ちに反映されます。

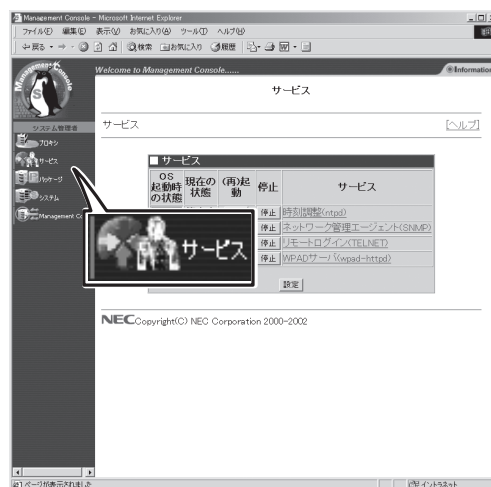
● **クライアント設定(クライアント追加/編集)**

クライアント別にポリシーの設定を行います。アクセス制限の対象となるクライアントのIPアドレスを設定し、指定したIPアドレスに対して適用したいポリシーの設定を行います。

サービス

システム管理者は、Management Consoleから以下サービスの設定を簡単に行うことができます。

- 時刻調整(ntpd)
- ネットワーク管理エージェント(SNMP)
- リモートログイン(TELNET)
- WPADサーバ(wpad-httpd)

サービス画面では各機能の停止・起動を指示可能で、現在の稼動状況を表示します。さらにここから、各機能ごとの詳細な設定を行う画面に移ります。

- OS起動時の状態:　本装置が起動した際に、このサービスを自動的に有効にするかどうかを指定します。
- 現在の状態:　現在、このサービスが動作しているかどうかを表示します。
- (再)起動:　このサービスが停止している場合に起動します。動作中の場合には、停止させてから再起動します。
- 停止:　このサービスが動作中であれば、停止します。

【サービスの画面構成】

■ サービス画面

- 時刻調整(ntpd)
  - 同期ホスト一覧
    - □ 時刻同期ホスト追加
    - □ 時刻同期状況の確認
- ネットワーク管理エージェント(SNMP)
  - コミュニティ一覧
    - □ コミュニティ追加
    - □ コミュニティ編集
  - システム情報
  - トラップ送信先一覧
    - □ トラップ送信先
- リモートログイン(TELNET)
  - TELNETログインを許可するホスト
- WPADサーバ(wpad-httpd)
  - プロキシサーバ自動設定ファイル

時刻調整(ntpd)

NTP(Network Time Protocol)は、ネットワークで接続されたコンピュータ同士が連絡を取り合い、時計のずれを自動的に調整する仕組みです。本装置はこの仕組みを利用して、以下の機能を提供しています。

- インターネットの標準時刻サーバに、本装置の時計を合わせる。
- 他のPCが時計を本装置に合わせるのに必要な情報を提供する。

【画面ごとの説明】

- **同期ホスト一覧**

本装置がNTPを使って連絡を取り合う標準時刻サーバあるいは PC(以降ホストと略記)の一覧を表示します。

■ 同期ホスト一覧

操作	タイプ	サーバ
追加		
削除	server	xx.xxx.xxx.xxx

時刻同期状況の確認

ー 追加

「時刻同期ホスト追加」画面に遷移します。

ー 削除

ボタンに対応するホストを一覧から削除します。

ー 時刻同期状況の確認

「時刻同期状況の確認」画面に遷移します。

- **時刻同期ホスト追加**

本装置がNTPを使って連絡を取り合うホストの追加登録を行います。

ー 別ホストと同期

ネットワークに接続されている他のホストと同期する場合に選択します。これが選択されている場合、以下が有効になります。

タイプ

server/peerのいずれかを指定します。

IPアドレス/ホスト名

ホストをIPアドレスあるいはホスト名で指定します。

- **時刻同期状況の確認**

登録されているホストとの間での時刻同期の状況を表示します。

■ 時刻同期状況の確認

remote	refid	st	t	when	poll	reach	delay	offset	jitter
xx.xxx.xxx	0.0.0.0	16	u	-	64		0.000	0.000	4000.00

ネットワーク管理エージェント(SNMP)

SNMP(Simple Network Management Protocol)は、ネットワークに接続された機器の稼動状況を、ネットワークを通じて取得するための仕組みです。本装置は、ネットワークに接続された機器(エージェント)の側として、必要な情報をネットワークに発信する機能を提供しています。

【画面ごとの説明】

● **コミュニティ一覧**

このネットワークエージェントにアクセス可能な管理マネージャマシンの一覧を表示します。またここから登録・変更・削除をします。

ー　追加

コミュニティを新規追加する画面に遷移します。

ー　編集

ボタンに対応するコミュニティの設定を変更する画面に遷移します。

ー　削除

ボタンに対応するコミュニティを一覧から削除します。

● **システム情報**

このマシンが設置されている場所や管理者のメールアドレスなどを記入しておいてください。この情報は必要に応じて管理マネージャから読み取られます(日本語を用いると、マネージャ側で文字が化けることがあります)。

● **トラップ送信先一覧**

このマシンに何らかの障害が発生した際に、トラップメッセージを送信する先(管理マネージャ)の一覧を登録します。

ー　追加

トラップ送信先を新規追加する画面に遷移します。

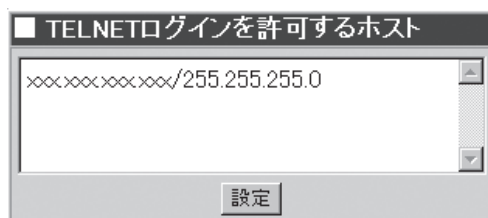
ー　編集

ボタンに対応するトラップ送信先の設定を変更する画面に遷移します。

ー　削除

ボタンに対応するトラップ送信先を一覧から削除します。

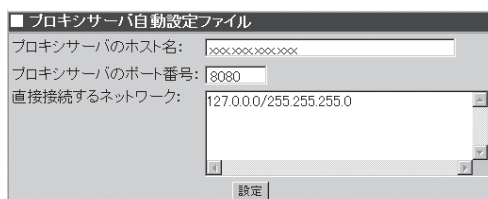
リモートログイン(telnet)

Management Consoleを使わずに他のコンピュータ(ホスト)から本装置に接続することを可能にする機能です。Management Consoleでは対応できない特別な操作を行いたい場合にだけこの機能を有効にします。通常の運用時に有効にする必要はありません。有効にしている間はセキュリティのレベルが低下しますので、通常は無効にしておくことをお勧めします。

TELNETログインを許可するホスト各種形式で、ログイン可能なホストを指定します。カンマで区切って複数のホストを指定可能です。IPアドレスやホスト名以外にも各種指定形式をサポートしています。指定形式の詳細についてはヘルプを参照してください。

重要

- **[システム]画面の[保守用パスワード]にてパスワードを設定後、「mainte」ユーザーでリモートログインが可能となります。**
- **本装置の初期設定時の「TELNETログインを許可するホスト」は「初期設定導入設定用ディスクで設定した本装置のIPアドレス/255.255.255.0」となります。**

WPADサーバ

本装置をフォワードプロキシとして利用している際に、ブラウザ側でのプロキシ設定を自動化するための機能です。Internet Explorer 5.5以降で対応しています。本機能を利用するためには、ブラウザの参照しているDNSサーバおよびDHCPサーバを適切に設定する必要があります。

[プロキシサーバ自動設定ファイル]画面で本装置に接続する際に使用するホスト名とポート番号を設定します。本装置を通さないで接続すべきマシンがあれば、ネットワークアドレス単位で指定することが可能です。

- **プロキシサーバのホスト名**

  ホスト名またはIPアドレスを指定します。

- **プロキシサーバのポート番号**

  ポート番号を指定します。

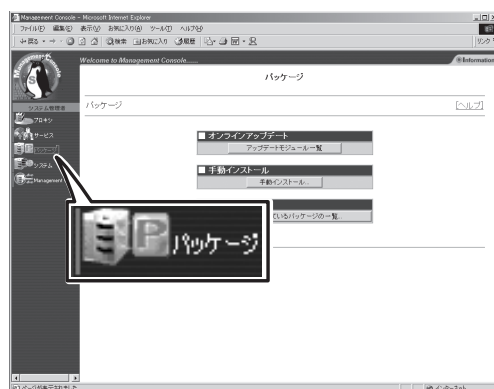
- **直接接続するネットワーク**

  ブラウザが本装置を経由しないで直接接続すべきネットワークを指定してください。

重要

WPADサーバは本装置のサーバ種別を「フォワード(透過型L4スイッチ)」、「フォワード(透過型WCCP)」または「リバース」に設定した時にはご利用できません。

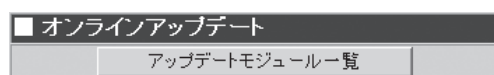
パッケージ

本装置にインストールされているアプリケーションなどのソフトウェアパッケージのアップデートやインストール、インストールされているパッケージの一覧を確認するページです。

オンラインアップデート

オンラインアップデートを利用すると、Management Consoleから安全にアップデートモジュールをインストールすることができます。

アップデートモジュールとは、本サーバに追加インストール(アップデート)可能なソフトウェアで、弊社で基本的な動作確認を行って公開しているものです。 内容は、既存ソフトウェアの出荷後に発見された不具合修正や機能追加などが主ですが、新規ソフトウェアが存在することもあります。オンラインアップデートでは、現在公開されている本サーバ向けのアップデートモジュールの一覧を参照し、安全にモジュールをインストールすることができます。

● **ユーザ認証**

初めてオンラインアップデートを利用する場合、また公開モジュールの最新情報を取得する場合、[ユーザ認証画面]が表示されます。ここで、基本サポートサービスをご購入されたお客様は、基本サポ ートサービスのお客様番号・分類・パスワードを入力してください。未購入のお客様は[認証しない]ボタンをクリックして進んでください。

■ ユーザ認証

基本サポートサービスを購入済みのお客様は、認証を行うことで購入者のみに公開されているアップデートモジュールを適用することができます。未購入のお客様は「認証しない」をクリックしてください。

お客様番号:

登録上の分類(1〜3):

パスワード:

送信　認証しない

アップデートモジュールのダウンロードログはシステムのログ管理の「Management Consoleログ」で確認することができます。

● アップデートモジュール一覧

公開されているアップデートモジュールの一覧が表示されます。本装置向けのモジュールで、まだインストールされていないモジュールのみが表示されます。各モジュールの機能や修正情報などを確認することができます。

■ アップデートモジュール一覧

日付	概要	パッケージ名	適用	操作
2000/xx/xx	telnet パッケージのアップデート [詳細情報]	telnet-0.17-xx	未	適用
2001/xx/xx	WPADサーバ修正モジュール [詳細情報]	wpad-httpd-1.00-xx	未	適用
2001/xx/xx	Management Console 機能強化モジュール [詳細情報]	wbmccache-1.0-xx	未	適用
2001/xx/xx	CacheServer カーネルアップデートモジュール [詳細情報]	kernel-2.4.3-xx roma-1.0-xx catfish-1.01-xx	未 未 未	適用

モジュールは、実際は主にRPMパッケージ形式で提供されるファイルですが、1つの機能のために複数のRPMパッケージを必要とする場合もあり、その場合は複数ファイルで構成されています。[適用]ボタンをクリックすると、該当モジュールのインストール作業を開始します。

● 信頼性の確認

「適用」ボタンをクリックすると、該当モジュールのインストールに必要なファイルをすべて取得します。ファイルのサイズが大きい場合は、時間がかかる場合があります。ファイルの取得が完了し、一時ディレクトリに保管した後、ファイルが正しく転送されたかどうかを自動的に検査します。検査にはMD5メッセージ・ダイジェストを用います。

検査に合格した場合は、画面に各ファイルのMD5メッセージ・ダイジェストが表示されます。最終的な確認として、弊社アップデートモジュール公開Webサイトで参照できる各ファイルのMD5メッセージ・ダイジェストの文字列と比較し、同じかどうか確認してください。[OK]ボタンをクリックするとインストールを実行します。

手動インストール

ローカルディレクトリのファイル名、またはURLを指定してRPMパッケージをインストールすることができます。詳細は画面上の[ヘルプ]をクリックしオンラインヘルプを参照してください。

■ 手動インストール

手動インストール...

● **ローカルディレクトリ指定**

本装置へCD-ROMからRPMパッケージをインストールしたい場合、CD-ROMドライブにRPMの入ったCD-ROMをセットし、この画面よりインストールしたいRPMパッケージを選んで追加してください。

● **URL指定**

本装置がすでにインターネットに接続されている場合には、RPMパッケージの置かれているサイトのURLを指定してそこからダウンロードしインストールを行うことができます。

重要

インストールする場合には、必ず[追加]ボタンをクリックしてください。

パッケージの一覧

現在本サーバにインストールされているRPMパッケージの一覧を確認することができます。また、アンインストール作業を行うこともできます。詳細は画面上の[ヘルプ]をクリックしオンラインヘルプを参照してください。

■ パッケージの一覧

インストールされているパッケージの一覧...

■ パッケージ一覧

グループ	パッケージ名	概要
Applications/Publishing	ghostscript-fonts-5.50-3	Fonts for the Ghostscript PostScript(TM) interpreter.
Documentation	indexhtml-7.1-2	The Web page you'll see after installing Red Hat Linux.
Applications/System	kon2-fonts-0.3.9b-6	Fonts for KON
System Environment/Base	mailcap-2.1.4-2	Associates helper applications with particular file types.
Documentation	man-pages-ja-0.4-3	Japanese man (manual) pages from the Linux Documentation Project
Development/Libraries	pump-devel-0.8.11-1	Development tools for sending dhcp requests
System Environment/Base	redhat-release-7.1-1	Red Hat Linux release file
System Environment/Base	filesystem-2.0.7-1	The basic directory layout for a Linux system.
System Environment/Libraries	glibc-2.2.2-10	The GNU libc libraries.
Development/Tools	byacc-1.9-18	A public domain Yacc parser generator.
Development/Tools	cproto-4.6-7	Generates function prototypes and variable declarations from C code.
Development/Tools	ctags-4.0.3-1	A C programming language indexing and/or cross-reference tool.
Development/Libraries	db1-devel-1.85-5	Development libs/header files for Berkeley DB (version 1) library.
Development/Libraries	db2-devel-2.4.14-5	Development libs/header files for Berkeley DB (version 2) library.
System Environment/Libraries	db3-devel-3.1.17-7	Development libraries/header files for the Berkeley DB library.
Applications/Communications	dip-3.3.7o-22	Handles the connections needed for dialup IP links.

システム

Management Console画面左の[システム]アイコンをクリックすると「システム」画面が表示されます。

システム停止／再起動

[システム]画面の[■システム停止／再起動]一覧から[システムの停止]、および[システムの再起動]を実行できます。

システムの停止

[システムの停止]ボタンをクリックすると「システムを停止します。よろしいですか?」とダイアログボックスが表示されます。停止する場合は[はい]ボタンを、停止したくない場合は[キャンセル]ボタンをクリックしてください。
[はい]ボタンをクリックすると、終了処理をした後、システムの電源がOFFになります。本体前面のPOWERランプが消灯したことを確認してください。

システムの再起動

[システムの再起動」ボタンをクリックすると「システムを再起動します。よろしいですか?」とメッセージが表示されます。再起動する場合は[はい]ボタンを、停止したくない場合は[キャンセル]ボタンをクリックしてください。
[はい]ボタンをクリックすると、終了処理をした後、システムがいったん停止し、再起動します。

状　態

［システム］画面の［■状態］一覧から以下のシステム状態を確認できます。

- **CPU/メモリ使用状況**

  メモリの使用状況とCPUの使用状況をグラフと数値で表示します。約10秒ごとに最新の情報に表示が更新されます。

- **ディスク使用状況**

  ディスクの使用状況を各ファイルシステムごとに数値とグラフで表示します。空き容量、使用率に注意してください。空き容量が足りなくなるとシステムが正常に動作しなくなる可能性があります。

- **プロセス実行状況**

  現在実行中のプロセスの一覧を表示します。プロセス実行状況の表の最上行の項目名をクリックすると、各項目で表示をソートすることができます。表示項目の詳細については、［ヘルプ］をクリックし、オンラインヘルプを参照してください。

- **名前解決診断**

  ネットワーク設定で登録されているDNSサーバの動作を確認することができます。
  「ホスト:」に適当なホスト名を入力して［診断］ボタンをクリックすると診断結果が表示されます。ホスト名に対して正しく「Name:」と「Address:」が表示されればDNSサーバは正常に機能しています。

- **ネットワーク利用状況**

  ネットワーク利用状況を表示します。
  ［約5秒毎に画面をリフレッシュする］チェックボックスをチェックすると自動的に表示が最新状況に更新されます。

- **ネットワーク接続状況**

  各ポートごとの接続状況を表示します。

  ［約5秒毎に画面をリフレッシュする］チェックボックスをチェックすると自動的に表示が最新状況に更新されます。

● **プロキシアクセス統計**

アクセスの統計情報を表示します。「Summary by Month」の表の[Month]の項目のリンクをクリックするとその月の詳細な統計情報を表示します。

■ プロキシアクセス統計表示

統計情報は作成されていません

■ プロキシアクセス統計設定

統計情報が以下のサイズを越えたら、情報をクリアします

10 MB （現時点では 統計情報は作成されていません）

設定

プロキシアクセス動作設定はプロキシアクセス統計を有効にして動作させるかどうか設定します。

動作させる際には優先度を設定してください。優先度は1から20まで設定可能であり、値が大きいほど優先度が低くなります。優先度を低くすることによりプロキシアクセス統計の動作によるCPUの負荷を減らすことができます。

Webalizer表示設定では、sitesはサイト別上位を、sites By KBytesはサイト別キロバイト上位を、URL'sはURL上位を、URL' s By KBytesはサイト別キロバイト上位をEntry Pagesは入り口上位を、Exit Pagesは出口別上位をいくつまで表示するか設定することができます。

- [初期設定]ボタンをクリックすると、それぞれのテキストボックスに初期値が入ります。
- 各テキストボックスは2桁まで入力することができます。
- 統計情報はCacheServerのアクセスログがローテートされたときに作成されます。
- CacheServerのアクセスログのローテートの設定は[システム]画面の[ログ管理]画面の[キャッシュサーバアクセスログ管理]にて行えます。

重要

- **プロキシアクセス統計を無効にするを選択するとそれまで作成されていた統計情報は削除されます。**
- **プロキシアクセス統計を動作させると性能低下がおこる可能性があります。**
- **優先度は慎重に決定してください。あまりに低い優先度を設定すると正常に動作しない可能性があります。**
- **プロキシアクセス統計情報を動作させると、キャッシュサーバのアクセスログのログ出力形式はSquidに、ローテート世代数は「1」に固定され、ローテートサイズはいったん100MBに設定されます。**
- **プロキシアクセス統計を動作させている時、ローテートサイズの扱いには注意してください。本装置の性能およびプロキシアクセス統計の動作に影響を与えます。**

● **経路情報**

「相手ホスト:」にホスト名を入力して[表示]ボタンをクリックすると、そのホストまでの経路情報を表示します。

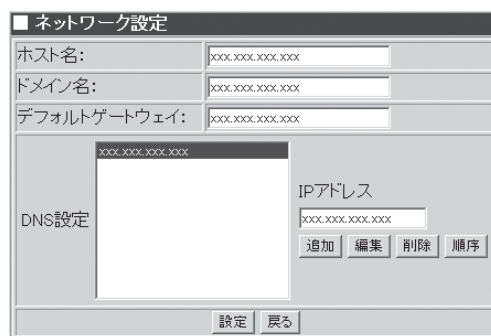
その他

［システム］画面の［■その他］一覧から、以下の機能を利用できます。

● **ネットワーク**

ホスト名、ドメイン名、デフォルトゲートウェイ、DNSの設定を行います。DNSは複数設定可能であり、順序を入れ替えることができます。

- DNSは16まで設定できます。
- DNSは上位に記述されているものを優先して使用します。

ここで設定されたDNSはRadius、Ldapの認証においても使用されます。

● **バックアップ**

ファイルのバックアップの設定を行います。バックアップに関してはこの後に説明する「バックアップ」を参照してください。

● **管理者パスワード**

管理者（admin）のパスワードそれぞれを変更します。また、管理者宛のメールを転送する先を設定できます。管理者宛メールの転送先は正しく送信できるアドレスを指定してください。

各パスワードは1文字以上8文字以下の半角英数文字（半角記号を含む）を指定してください。省略すると、パスワードは変更されません（空のパスワードを指定することはできません）。

● アクセスログ取得

本装置のアクセスログをSambaまたはFTPで指定したホストを転送します。

アクセスログ取得を動作させる際には優先度を設定してください。優先度は1から20まで設定可能であり、値が大きいほど優先度が低くなります。優先度を低くすることによりアクセスログ取得の動作によるCPUの負荷を減らすことができます。

重要

- **アクセスログ取得を行っている時、[システム]画面の[ログ管理]画面のキャッシュサーバアクセスログのログの世代数は「1」に固定されます。**
- **アクセスログ取得やプロキシアクセス統計情報を動作させている時はローテートサイズの扱いに注意してください。本装置の性能に影響を与えます。**
- **アクセスログ取得を動作させると性能低下がおこる可能性があります。**
- **優先度は慎重に決定してください。あまりに低い優先度を設定すると正常に動作しない可能性があります。**
- **アクセスログの転送はログのローテートが行われるタイミングで実行されます。**
- **アクセスログのローテートサイズの指定は[システム]画面の[ログ管理]画面の[キャッシュサーバアクセスログ設定]にて行えます。**

● プロキシサーバ状態表示

[システム]画面の[プロキシサーバ状態表示]では、本装置に関するさまざまな情報を確認することができます。

キャッシュサーバのメジャーバージョン	1
キャッシュサーバのマイナーバージョン	0
キャッシュサーバのOEMバージョン	1125
キャッシュサーバの総メモリサイズ	512 MB
キャッシュサーバのキャッシュディスクサイズ	3662 MB
最後にキャッシュサーバが起動された時間	2001.11.29 21:42:32
最後にキャッシュサーバが起動されてからの合計稼動時間	1:1:30

[プロキシサーバ状態表示]画面は、以下の7つに分類され、それぞれのボタンをクリックすることで、関連する詳細な情報を確認できます。また、それぞれの画面は一定時間ごとに最新情報に更新されます。

－ 一般情報

[一般情報]ボタンをクリックすると、[プロキシサーバ状態表示(一般情報)]画面が表示されます。この画面では、システムのバージョン情報や、運用時間等を確認することができます。

－ キャッシュ概要

[キャッシュ概要]ボタンをクリックすると、[プロキシサーバ状態表示(キャッシュ概要)]画面が表示されます。この画面では、システムの現在の動作状況等を確認することができます。

- キャッシュ情報

  [キャッシュ情報]ボタンをクリックすると、[プロキシサーバ状態表示(キャッシュ情報)]画面が表示されます。この画面では、一定時間あたりの本装置への接続数や、リクエスト数等を確認することができます。

- クライアント要求

  [クライアント要求]ボタンをクリックすると、[プロキシサーバ状態表示(クライアント要求)]画面が表示されます。この画面では、システムが起動開始から現時点までに処理したさまざまな情報を確認することができます。

- ICP情報

  [ICP情報]ボタンをクリックすると、[プロキシサーバ状態表示(ICP情報)]画面が表示されます。この画面では、隣接サーバと関連する情報を確認することができます。

- CERN情報

  [CERN情報]ボタンをクリックすると、[プロキシサーバ状態表示(CERN情報)]画面が表示されます。この画面では、親サーバと関連する情報を確認することができます。

- FTP情報

  [FTP情報]ボタンをクリックすると、[プロキシサーバ状態表示(FTP情報)]画面が表示されます。この画面では、FTPプロトコルに関する情報を確認することができます。

● **ログ管理**

ログの表示、ログのローテートの設定を行います。

ログの表示は表示したいログの[表示]ボタンをクリックするとローテートされたログの一覧が表示され、その中から表示したいログを選択して表示します。

ログのローテートの設定は、ローテートを行うタイミングを周期またはローテートサイズで指定し、何世代までログを残すかを設定します。

■ ログ管理

操作		ログファイル	ローテート	世代
表示	設定	キャッシュサーバアクセスログ		
表示	設定	システムログ		
表示	設定	システムのセキュリティログ		
表示	設定	システムのメールログ		
表示	設定	システムのブートログ		
表示	設定	クーロンログ		
表示	設定	WPADサーバログ		
表示	設定	WCCPログ		
表示	設定	Management Consoleログ	毎週	5
表示	設定	Management Consoleのアクセスログ		
表示	設定	Management Consoleのエージェントログ		
表示	設定	Management Consoleのエラーログ		
表示	設定	Management Consoleの参照ログ		
表示	設定	Management ConsoleのSSLリクエストログ		

ログを表示したとき、ログのダウンロードを行うことも可能です。

重要

- **ログのローテートは毎日0:00とマシン起動時にチェックし、条件があっているものをローテートします。**
- **ログのローテートのタイミングでマシンの停止および再起動を行う場合にはご注意ください。**
- **本装置のアクセスログの設定は他のログと異なります。詳細は後に説明する「キャッシュサーバアクセスログ設定」を参照してください。**

－　キャッシュサーバアクセスログ管理

本装置のアクセスログの出力形式、ローテートサイズ、何世代までログを残すかなどを設定します。出力形式が拡張形式であったとき、拡張形式でチェックボックスにチェックを入れた項目がログ出力されます。

重要

- **プロキシアクセス統計情報を有効にしている時は出力形式はSquid、世代数は「1」に固定され、ローテートサイズはいったん100MBに設定されます。**
- **本装置のアクセスログ管理を行っている時、世代数は「1」に固定されます。**
- **本装置のアクセスログ管理やプロキシアクセス統計情報を動作させている時はローテートサイズの扱いに注意してください。本装置の性能に影響を与えます。**

アクセスログのフォーマット

アクセスログは、2つの形式から選択し、出力することができます。それぞれの出力内容は以下のようになります。

- Squid形式

出力例: 989605543.072 89 xxx.xxx.xxx.xxx TCP HIT/200 7653 GET http://www.foobar.com/ - DIRECT/proxy.xxx.xx.jp text/html
①989605543.072 ②89 ③xxx.xxx.xxx.xxx ④TCP HIT/200 ⑤7653 ⑥GET ⑦http://www.foobar.com/ ⑧- ⑨DIRECT/proxy.xxx.xx.jp ⑩text/html

各出力項目を説明します。

① タイムスタンプ － データオブジェクトの取得処理が完了した時間です。UNIX時間(1970年1月1日からの秒数)で出力します。
② 経過時間 － データオブジェクトの取得処理にかかった時間をミリ秒で出力します。
③ クライアントアドレス － クライアントのIPアドレスを出力します。
④ ログタグ／HTTPコード番号 － CacheServerがどのように要求を処理したかを表すタグ名と、HTTPのステータスコードを出力します。
⑤ サイズ － データオブジェクトのサイズをバイトで出力します。
⑥ 要求方法 － HTTPの要求方法を出力します。
⑦ URL － 要求されたURLを出力します。
⑧ 出力無し － 必ず「ー」が出力されます。
⑨ 階層構造データタグ/ホスト名 － オブジェクトの取得がどのように行われたかを表すタグ名と、取得したサーバ名を出力します。
⑩ コンテンツタイプ － オブジェクトデータのコンテンツタイプを出力します。

● 拡張形式

出力例: 2001-12-04 16:34:36 xx.xx.xx.xx - yy.yy.yy.yy sss GET http://www.foobar.com/ - - HTTP/1.0 200 837 147 188 "AAA/Browser(aaa)" "" "" HIT - -

(① 2001-12-04 16:34:36 ② xx.xx.xx.xx ③ - ④ yy.yy.yy.yy ⑤ sss ⑥ GET ⑦ http://www.foobar.com/ ⑧ - ⑨ - ⑩ HTTP/1.0 ⑪ 200 ⑫ 837 ⑬ 147 ⑭ 188 ⑮ "AAA/Browser(aaa)" ⑯ "" ⑰ "" ⑱ HIT ⑲ - ⑳ -)

各出力項目を説明します。

① 日付と時刻
② クライアントのIPアドレス
③ ユーザー名(認証機能を使用した時のみ出力されます)
④ CacheServerのIPアドレス
⑤ リバースプロキシ動作時のホスト名(またはIPアドレス)
⑥ HTTPの要求方法
⑦ URL
⑧ URLステム ー URLに「?」が含まれた場合、「?」までのURLを出力します。
⑨ URLクエリー ー URLに「?」が含まれた場合、「?」以降のURLを出力します。
⑩ HTTPバージョン
⑪ HTTPステータスコード
⑫ データオブジェクトサイズ(バイト)
⑬ リクエストサイズ(バイト)
⑭ 経過時間
⑮ ユーザーが使用したブラウザ情報
⑯ 参照URL
⑰ 発信元クライアントIPアドレス
⑱ キャッシュHIT/MISS
⑲ 連携プロキシIPアドレス ー プロキシ階層がある場合は、リクエストを送信した連携プロキシのIPアドレスを出力します。
⑳ WEBサーバIPアドレス ー プロキシ階層が無い場合は、リクエストを送信したWEBサーバのIPアドレスを出力します。

*1 ③〜⑳の項目は、出力の有無をユーザーが選択することが可能です。
*2 詳細な説明は、オンラインヘルプを参照してください。

● **時刻設定**

システムの時刻を設定できます。[設定]ボタンをクリックすると、現在入力している時刻がシステムに設定されます。

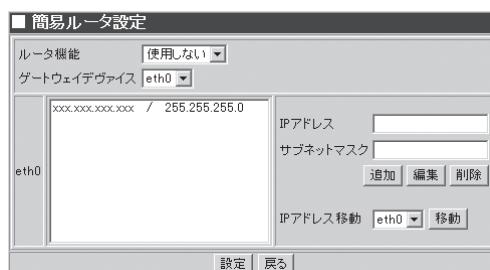
● **保守用パスワード**

保守用ユーザー(mainte)のパスワードを設定します。設定後、「mainte」ユーザーでリモートログイン(telnet)サービスを利用することができます。パスワードは6文字以上8文字以下の半角英数字(半角記号を含む)を指定してください。省略するとパスワードは変更されません。また空のパスワードを指定することはできません。

● **簡易ルータ設定**

本装置では複数のネットワークポートを利用できます。

これらポートそれぞれに、複数のIPアドレスを割り当てて、複数のネットワークに所属させることが可能となっています。

ネットワークポートごとに、現在割り当てられているIPアドレス/サブネットマスクの一覧を表示します。また、ここから追加・編集・削除操作を行います。

— ルータ機能

ルータ機能の使用・不使用を指定します。

— IPアドレス

追加・修正するIPアドレスを入力します。

— サブネットマスク

IPアドレスが所属するネットワークのサブネットマスクを入力します。

— ゲートウェイデバイス

ゲートウェイデバイスを指定します。

— IPアドレス移動

一覧にて選択したIPアドレスを他のネットワークインターフェースに移動します。

重要

- **サーバ種別にフォワード(透過型L4スイッチ)、フォワード(透過型WCCP)が設定されていて、バイパス設定に設定が存在するときルータ機能が自動で「使用する」になります。**
- **上記の状態以外になった時、ルータ機能の設定は元に戻りますが、上記の状態中に簡易ルータ設定画面で「設定」ボタンをクリックすると、簡易ルータ設定を使用する意志が無くても使用するに設定したと見なされます。**
- **サーバ種別にフォワード(透過型L4スイッチ)やフォワード(透過型WCCP)が設定されていて、バイパス設定に設定が存在するときルータ機能で「使用しない」を指定できません。**

バックアップ

システムの故障、設定の誤った変更など思わぬトラブルからスムーズに復旧するために、定期的にシステムのファイルのバックアップをとっておくことを強く推奨します。
バックアップしておいたファイルを「リストア」することによってバックアップを作成した時点の状態へシステムを復元することができるようになります。
本装置では、システム内のファイルを以下の4つのグループに分類して、その各グループごとにファイルのバックアップのとり方を制御することができます。

- システムの設定ファイル
- プロキシサーバの設定ファイル
- 各種ログファイル
- プロキシアクセス統計情報

初期状態では、いずれのグループも「バックアップしない」設定になっています。お客様の環境にあわせて各グループのファイルのバックアップを設定してください。
本装置では各グループに対して「ローカルディスク」と「Samba」の2種類のバックアップ方法を指定することができます。
各方法には、それぞれ以下のような特徴があります。

- **ローカルディスク**

  内蔵ハードディスクの別の場所にバックアップをとります。

- Samba

  LANに接続されているWindowsマシンのディスクにバックアップをとります。

重要

- **システムの設定ファイル、およびプロキシサーバの設定ファイルは必ずバックアップを設定してください。**
- **ローカルディスクへのバックアップは、他の方法に比べてリストアできない可能性が高くなります。なるべくSambaを使用して、別マシンへバックアップをとるようにしてください。**
- **Sambaでのバックアップは、内蔵ハードディスクがクラッシュしても復元を行うことができますが、あらかじめ、Windowsマシンに共有の設定をしておく必要がありますので注意してください。**
- **プロキシのアクセスログおよびキャッシュログは、「各種ログファイル」のバックアップでの対象外となります。注意してください。**

「Samba」によるバックアップ設定の例

ここでは「Samba」を使用したバックアップの方法について説明します。
例としてマシン名「winpc」というWindowsマシンの「C:ドライブ」にバックアップのためのフォルダ「cachebackup」を作成して「システム、各種サーバの設定ファイル」グループのファイルのバックアップを行う場合の操作手順を説明します。
バックアップファイルを置くマシン（winpc）でのバックアップ作業のためのユーザーを「winpc」上にあらかじめ用意してください。

重要 **バックアップファイルの中にはシステムのセキュリティに関する情報などが含まれるため、バックアップのためのフォルダ（cachebackup）の読み取り、変更の権限などのセキュリティの設定には十分注意してください。（Windows Me/98/95ではセキュリティの設定ができません。そのためお客様の情報が利用者に盗まれる可能性があります。）**

バックアップ作業のためのユーザーは既存のユーザーでもかまいませんが、以下の説明では「cacheadmin」というユーザーをあらかじめ用意したという前提で説明します。

次の順序で設定します。以降、順に設定例を説明していきます。

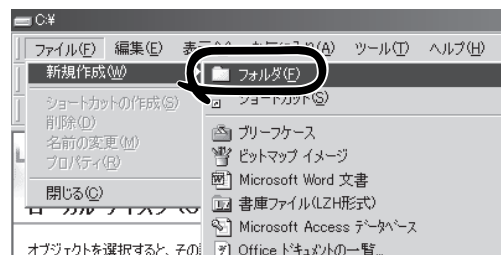
1. Windowsマシンの共有フォルダの作成
2. システムのバックアップファイルグループの設定
3. バックアップの実行

バックアップ用に作成した共有フォルダの設定を不用意に変更するとシステムのバックアップおよび復元の機能が正常に動作しなくなるので注意してください。

Windowsマシンの共有フォルダの作成

まず、バックアップファイルを置いておくための共有フォルダをWindowsマシンに作成します。ここでは、例としてWindows 2000、Windows NT、Windows 98の3種のOSでの作成方法を説明します。

操作例：winpcのOSがWindows 2000の場合

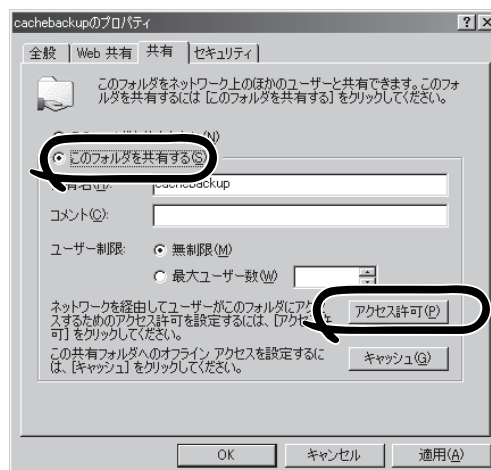
1. マシン「winpc」のデスクトップ上にある［マイコンピュータ］をダブルクリックする。
2. 開いた［マイコンピュータ］ウィンドウの［C：ドライブ］のアイコンをダブルクリックする。
3. ［ファイル］メニューの［新規作成］→［フォルダ］をクリックする。

4. [新しいフォルダ]の名前に[cachebackup]とキーボードから入力し<Enter>キーを押す。

5. 上記の手順で作成した[cachebackup]フォルダをクリックして選択する。

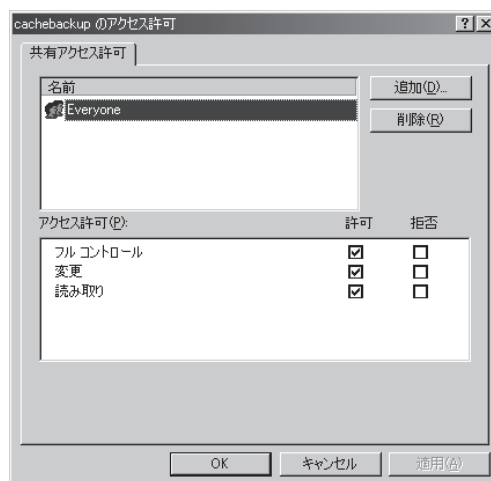
6. [ファイル]メニューの[共有]をクリックする。

   [cachebackupのプロパティ]ウィンドウの[共有]シートが表示されます。

7. [このフォルダを共有する]をクリックする。

8. [アクセス許可]ボタンをクリックする。

9. [共有アクセス許可]を設定する。

   ここでは以下のように設定します。

   1. [名前]一覧から[Everyone]を削除する。
   2. [追加]ボタンをクリックして[ユーザー、コンピューター、またはグループの選択]ウィンドウでユーザー[cacheadmin]を追加して[OK]ボタンをクリックする。
   3. [共有アクセス許可]の[アクセス許可]一覧の[フルコントロール]の許可のチェックボックスにチェックをつける。

10. [OK]ボタンをクリックして[cachebackupのアクセス許可]のウィンドウを閉じる。

11. [OK]ボタンをクリックして[cachebackupのプロパティ]のウィンドウを閉じる。

12. [cachebackup]フォルダのアイコンが変わったことを確認する。

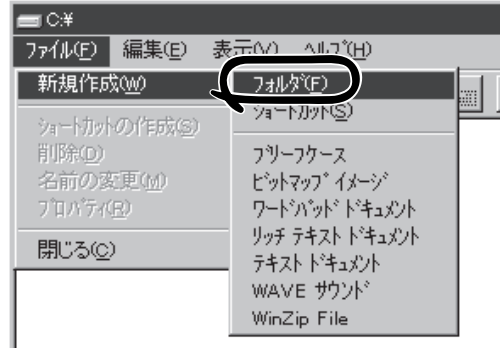
以上でWindows上の共有フォルダの設定は完了です。

操作例：winpcのOSがWindows NTの場合

1. マシン「winpc」のデスクトップ上にある[マイコンピュータ]をダブルクリックする。

2. 開いた[マイコンピュータ]ウィンドウの[C:ドライブ]のアイコンをダブルクリックする。

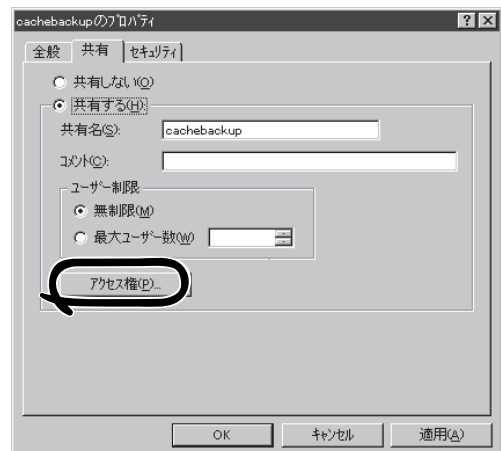
3. [ファイル]メニューの[新規作成]→[フォルダ]をクリックする。

4. [新しいフォルダ]の名前に[cachebackup]とキーボードから入力し<Enter>キーを押す。

5. 上記の手順で作成した[cachebackup]フォルダをクリックして選択する。

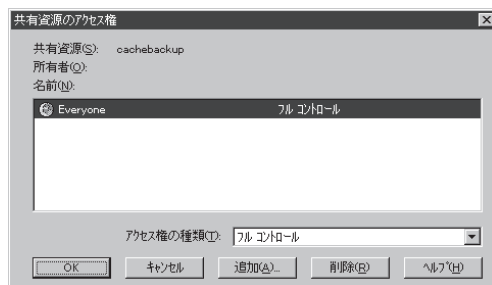
6. [ファイル]メニューの[共有]をクリックする。

   [cachebackupのプロパティ]ウィンドウの[共有]シートが表示されます。

7. [共有する]をクリックする。

8. [アクセス権]ボタンをクリックする。

9. [共有資源のアクセス権]を設定する。

   ここでは以下のように設定します。

   1. [名前]一覧から[Everyone]を削除する。
   2. [追加]ボタンをクリックして[ユーザーとグループの追加]ウィンドウで[ユーザーの表示]ボタンをクリックしてユーザー[cacheadmin]を選択して[追加]ボタンをクリックする。
   3. [アクセス権の種類]のプルダウンメニューから[フルコントロール]を選択して[OK]する。

10. [OK]ボタンをクリックして[共有資源のアクセス権]のウィンドウを閉じる。

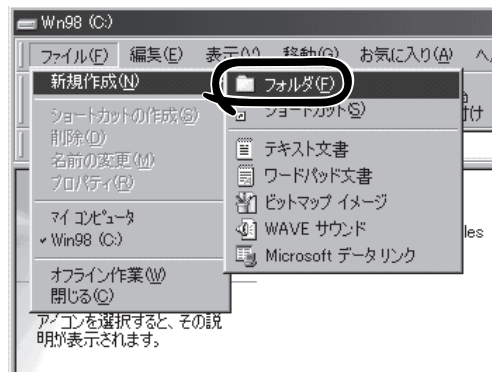
11. [OK]ボタンをクリックして[cachebackupのプロパティ]のウィンドウを閉じる。

以上でWindows NT上の共有フォルダの設定は完了です。

操作例：winpcのOSがWindows 98の場合

1. マシン「winpc」のデスクトップ上にある[マイコンピュータ]をダブルクリックする。

2. 開いた[マイコンピュータ]ウィンドウの[C:ドライブ]のアイコンをダブルクリックする。

3. [ファイル]メニューの[新規作成]→[フォルダ]をクリックする。

4. [新しいフォルダ]の名前に[cachebackup]とキーボードから入力し<Enter>キーを押す。

5. 上記の手順で作成した[cachebackup]フォルダをクリックして選択する。

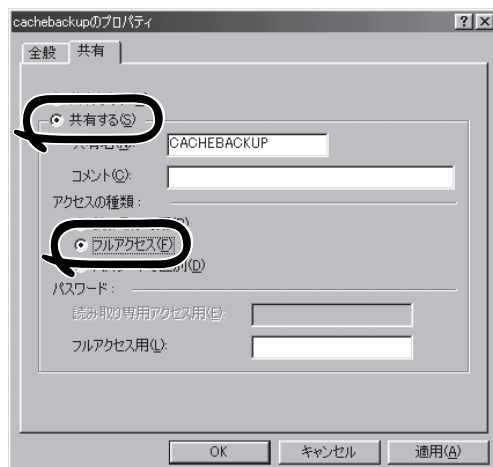
6. [ファイル]メニューの[共有]をクリックする。

   [cachebackupのプロパティ]ウィンドウの[共有]シートが表示されます。

7. [共有する]をクリックする。

8. [アクセスの種類]で[フルアクセス]をクリックする。

> **重要**
>
> **[パスワード]の[フルアクセス用]欄には何も設定しないでください。**

9. [ＯＫ]ボタンをクリックして[cachebackupのプロパティ]のウィンドウを閉じる。

以上でWindows 98上の共有フォルダの設定は完了です。

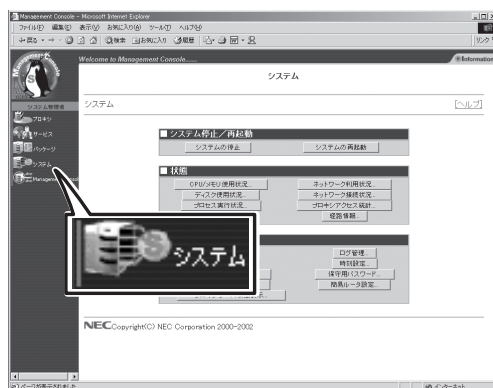
システムのバックアップファイルグループの設定

ここでは例として[システム、各種サーバの設定ファイル]グループのバックアップの設定手順を説明します(他のグループも操作方法は同じです)。

1. Management Console画面左の[システム]アイコンをクリックする。

   [システム]画面が表示されます。

2. [システム]画面の[■その他]一覧の[バックアップ]ボタンをクリックする。

   バックアップの設定画面が表示されます。

3. 一覧の[システム、各種サーバの設定ファイル]の左側の[編集]ボタンをクリックする。

   バックアップ設定の[編集]画面が表示されます。

■ バックアップ一覧

操作	説明	世代数	タイミング
編集	システムの設定ファイル	5	バックアップしない
編集	プロキシサーバの設定ファイル	5	バックアップしない
編集	各種ログファイル	5	バックアップしない
編集	プロキシアクセス統計情報	5	バックアップしない

4. [編集]画面のバックアップ方式の[Samba]をクリックして選択する。

5. 「Windowsマシンの共有フォルダの作成」で行った設定に従って以下の項目を入力する。

- [Windowsマシン名]: winpc
- [共有名]:0000 cachebackup
- [ユーザ名]: cacheadmin
- [パスワード]:cacheadminのパスワード

6. 正しく設定されていることを確認するため[即実行]ボタンをクリックしてバックアップを実行する。

   正しく実行された場合は以下の操作結果通知が表示されます。

正しく操作結果通知が表示されない場合はWindowsマシンの共有の設定とバックアップ方式の設定が正しいかどうか確認してください。

ヒント

この[即実行]ボタンを使うことで、任意のタイミングで手動でバックアップを行うことができます。

7. [戻る]ボタンをクリックする。

定期的に自動的にバックアップを行うには次の設定を続けて行ってください。

8. [編集]画面で[世代]、[スケジュール]、[時刻]を指定する。

右図の例では[毎週月曜日の朝9:00にバックアップをとる。バックアップファイルは3世代分残す]設定を行う場合を示しています。

世代

バックアップファイルをいくつ残すかを指定します。バックアップファイルを保管するディスクの容量と、必要性に応じて指定してください。世代を1にすると、バックアップを実行するたびに前回のバックアップ内容を上書きすることになります。

スケジュール

バックアップを実行する日を指定します。[毎日]、[毎週]、[毎月]、および[バックアップしない]から選択します。

[毎週]を指定する場合は右側の曜日も選択してください。

[毎月]を指定する場合は右側のテキストボックスに日付を入力してください

いずれの場合も指定した日付に本体の電源とバックアップ先のマシンの電源が入っていない場合はバックアップできないので注意してください。

時刻

[スケジュール]で指定した日付の何時何分にバックアップを行うかを指定します。指定した時刻に本体の電源とバックアップ先のマシンの電源がONになっていない場合はバックアップできないので注意してください。

9. [編集]画面下の[設定]ボタンをクリックする。

以上で、定期的に自動的にバックアップを行う設定は完了です。

バックアップの実行

バックアップの処理は「システムのバックアップファイルグループの設定」で指定した日時に本体の電源とバックアップ先のマシンの電源が入っていない場合は、バックアップされませんので注意してください。

リストア

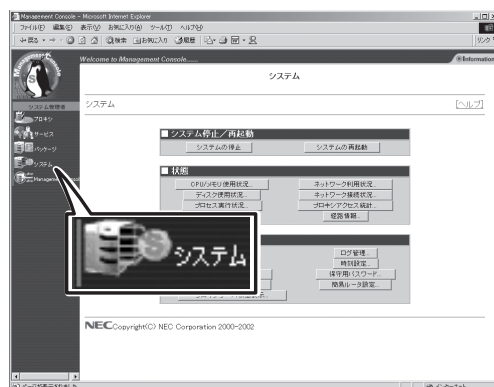
バックアップファイルは4つの各バックアップファイルグループごとにシステムにリストアすることができます。

ここでは例として[バックアップ手順の例]で設定を行った[システム、各種サーバの設定ファイル]グループのファイルのバックアップファイルをシステムにリストアする際の操作手順の例を説明します。

1. Management Console画面左の[システム]アイコンをクリックする。

   [システム]画面が表示されます。

2. [システム]画面の[■その他]一覧の[バックアップ]ボタンをクリックする。

   バックアップの設定画面が表示されます。

3. 一覧の[システム、各種サーバの設定ファイル]の左側の[編集]ボタンをクリックする。

   バックアップの設定をする[編集]画面が表示されます。

■ バックアップ一覧

操作	説明	世代数	タイミング
編集	システムの設定ファイル	5	バックアップしない
編集	プロキシサーバの設定ファイル	5	バックアップしない
編集	各種ログファイル	5	バックアップしない
編集	プロキシアクセス統計情報	5	バックアップしない

4. [編集]画面の下の方にある[リストア]ボタンをクリックする。

   リストアするバックアップファイルの一覧が表示されます(一覧には最大で[世代数]の数だけファイルが表示されます)。

5. 一覧からリストアしたいバックアップファイルを選択して[リストア]ボタンをクリックする。

   通常は、デフォルトで最も新しいバックアップファイルが選択されています。そのまま[リストア]ボタンをクリックすれば最新のバックアップがリストアされます。

   [リストアします。よろしいですか?]というダイアログボックスが表示されます。

■ リストア

バックアップ方式 : Samba

リストアするバックアップファイル

	バックアップ項目
○	backup_smb_conf_0.tgz A 889877 Wed Nov 8 10:00:11 2000
○	backup_smb_conf_1.tgz A 889877 Wed Nov 15 10:00:13 2000
◉	backup_smb_conf_2.tgz A 889877 Wed Nov 22 10:00:12 2000

表示 リストア

6. リストアする場合には[OK]ボタンをクリックする。

   リストアをしない場合には[キャンセル]ボタンをクリックしてください。